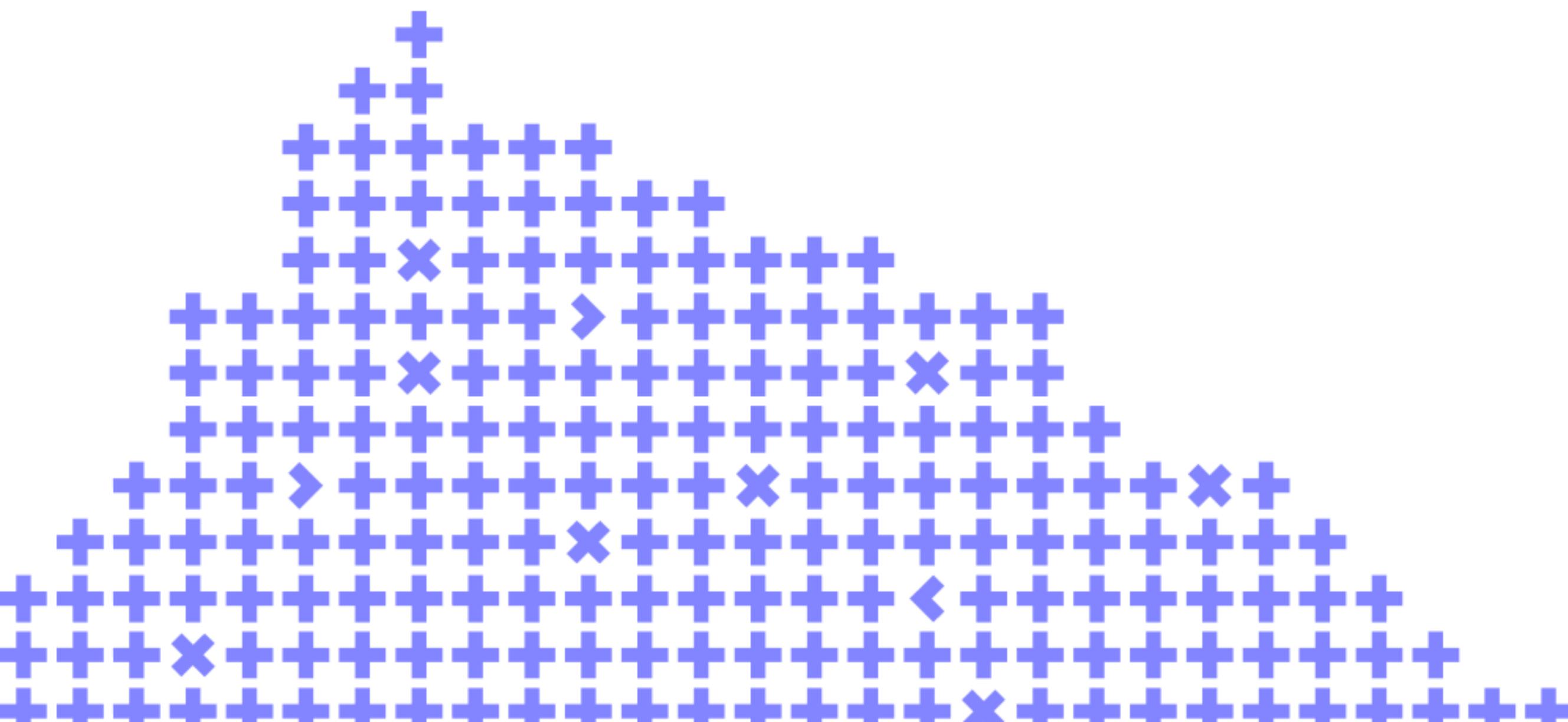


The clashes of the titans – Usability vs. Security. Can they live together?

Alon Kiriati



Co-organizer

Yandex





[Home](#) > [Scotland](#) > [Supporters & Tickets](#) > [Scotland Tickets](#)

/ [Hospitality](#)

/ [Membership](#)

/ [News](#)

/ [Newsletter](#)

BUY SCOTLAND TICKETS

Keep up to date with the latest ticketing news via [Scotland National Team Twitter](#) and [Scotland National Team Facebook](#).

Scotland v Ukraine

F.I.F.A. World Cup Play-off | A Squad

24/03/2022 7:45pm Glasgow

[BUY ONLINE](#)



Ticket Office

[Buy Online](#)



Scotland v Ukraine

F.I.F.A. World Cup Play-off | [A Squad](#)



24/03/2022 7:45pm Glasgow

[BUY ONLINE](#)

SCOTLAND MEN'S NATIONAL FOOTBALL TEAM

HOME MATCH PACKAGE 2022

Home Match Package 2022

Thursday, 24 March, 2022 - Friday, 23 September, 2022

CAN I BUY THIS PRODUCT?

You need to have purchased or have in your basket [Scotland Supporters Club 2020-2021](#) before buying this!

IMPORTANT INFORMATION

Package Includes - *FIFA World Cup Play Off - Scotland v Ukraine *UEFA Nations League - Scotland v Armenia *UEFA Nations League - Scotland v Ukraine *UEFA Nations League - Scotland v Republic of Ireland

[Select Seats](#)



REGISTER NEW ACCOUNT

If you are a new customer who has never purchased tickets from The Scottish FA before, please click the 'Register New Account' button and register online now.

[Register New Account](#)



Tickets

MENS 'A' HOME GAMES

Find home tickets for upcoming Scotland Men's National Football Team.

[BUY TICKETS](#)

PERSONAL DETAILS (WHO THE MEMBERSHIP IS FOR)

Title*

Forename*

Surname*

Date of Birth*

Sex*

Email*



PASSWORD

(Passwords need be 8-64 characters long and contain 1 upper case letter, 3 lower case letters, 1 number and 1 special character e.g !@#£%)

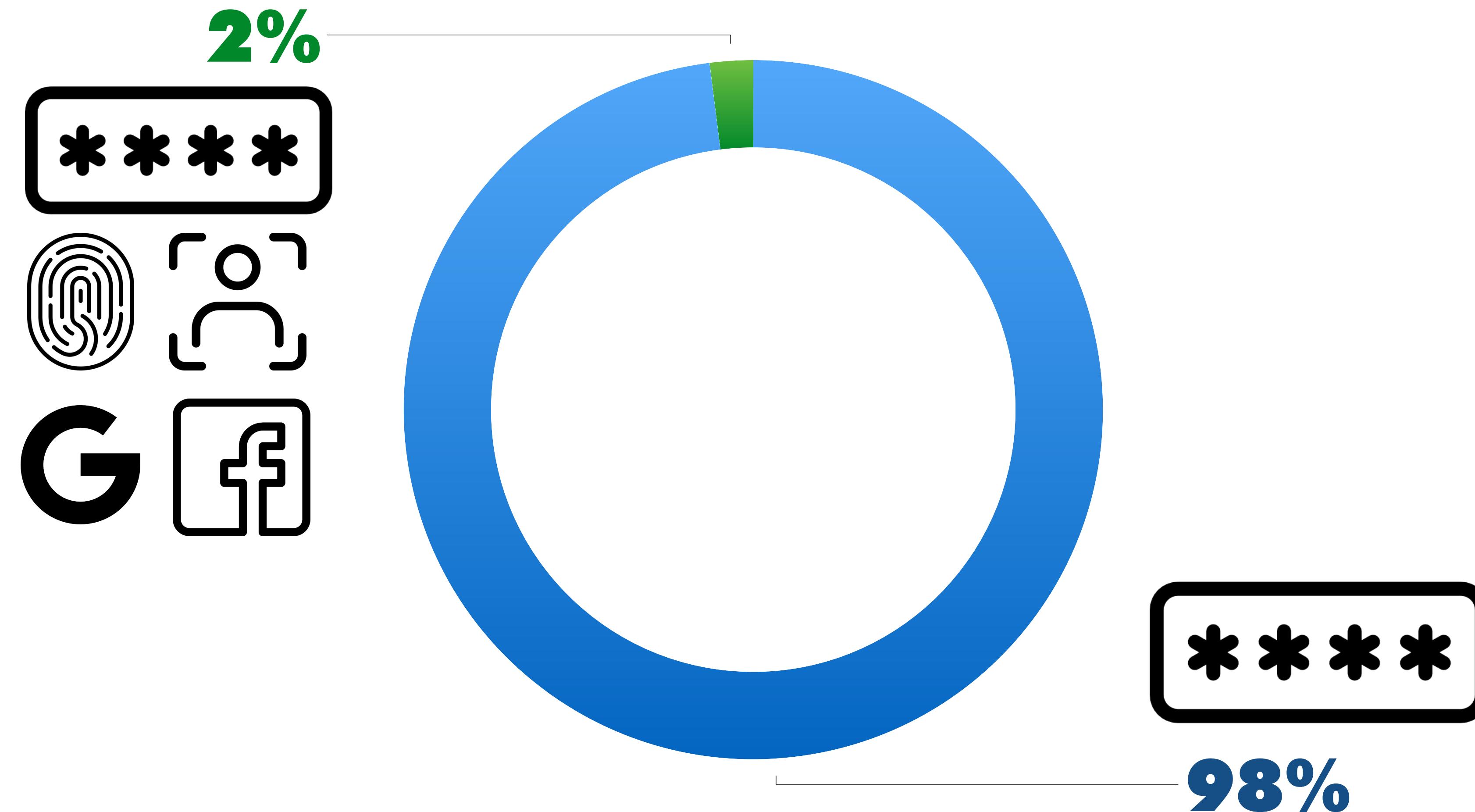
Password*



Confirm Password*



IS IT STILL 1990?



DATA BREACHES

2.7B



\$2.1T



IF IT HAPPENED TO THEM, IT CAN HAPPEN TO YOU



2020 / 200M users



2019 / 540M users



2019 / 250M users



2017 / 57M users

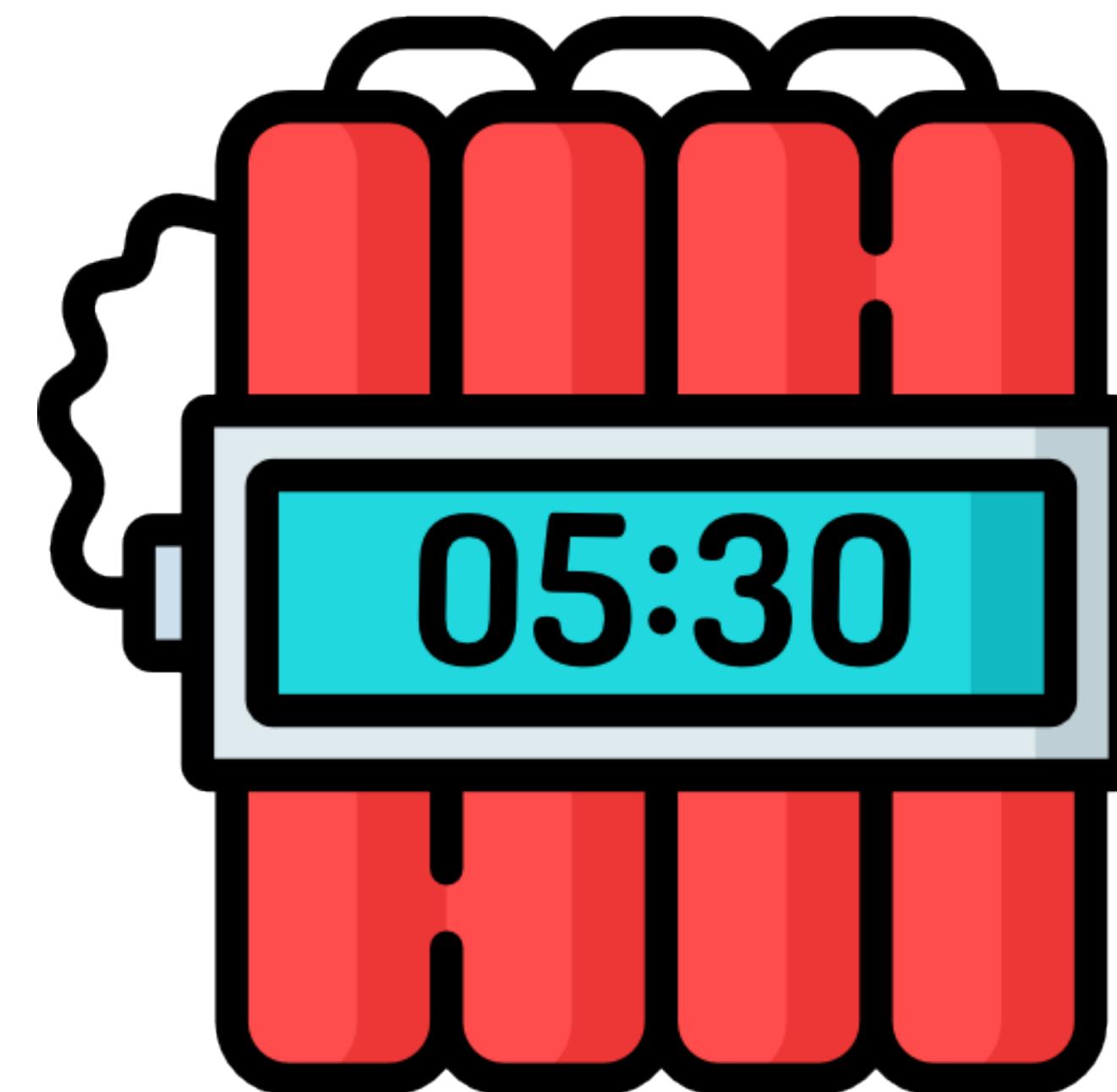


2012 / 12M users



2013 / 4.7M users

YOUR LAST LINE OF PROTECTION

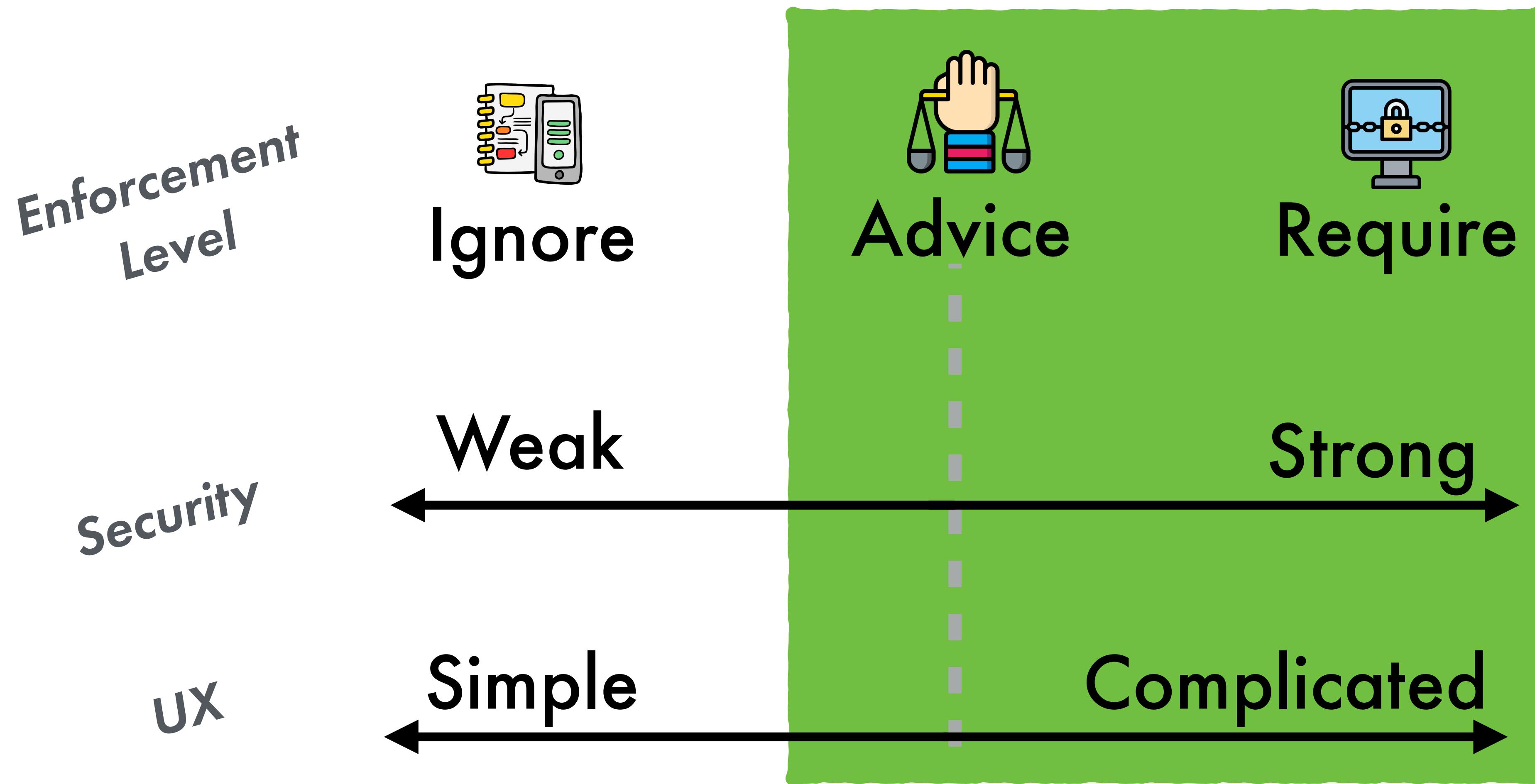


a3N ^ g5%7*xR



123456

UX / SECURITY TRADEOFFS



#1 BUILD

Where You're Logged In

	Chrome · Active now	
	Messenger · 5 hours ago	

▼ See More

Login

	Change password It's a good idea to use a strong password that you're not using elsewhere	
	Save your login info On • It will only be saved on the browsers and devices you choose	

Two-factor authentication

	Use two-factor authentication We'll ask for a login code if we notice an attempted login from an unrecognized device or browser.	
	Authorized Logins Review a list of devices where you won't have to use a login code	

Setting Up Extra Security

	Get alerts about unrecognized logins On • We'll let you know if anyone logs in from a device or browser you don't usually use	
	Choose 3 to 5 friends to contact if you get locked out Your trusted contacts can send a code and URL from Facebook to help you log back in	

Advanced

	Encrypted notification emails Add extra security to notification emails from Facebook (only you can decrypt these emails)	
	See recent emails from Facebook See a list of emails we sent you recently, including emails about security	

#1 BUILD

Logins

Password estimation

2-factor authentication

Sessions control

Sign-in every X days

Idle time

Device/web control

Connected Devices

Web Sessions

Alerts

New sign-ins

Suspicious activity

Recovery

Recovery mail

Recovery codes

Data control

3rd party apps

Encryption method

#1 BUILD

Security

Require that all meetings are secured with one security option



Require that all meetings are secured with one of the following security options: a passcode, Waiting Room, or "Only authenticated users can join meetings". If no security option is enabled, Zoom will secure all meetings with Waiting Room. [Learn more](#) 

Waiting Room



When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

Waiting Room Options

The options you select here apply to meetings hosted by users who turned 'Waiting Room' on

- ✓ Users who are not in your account and not part of your whitelisted domains will go in the waiting room
- ✓ Host, co-hosts, and anyone who bypassed the waiting room (only if host and co-hosts are not present) can admit participants from the waiting room

[Edit Options](#) [Customize Waiting Room](#)

Require a passcode when scheduling new meetings



A passcode will be generated when scheduling a meeting and participants require the passcode to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

Require a passcode for instant meetings



A random passcode will be generated when starting an instant meeting

Require a passcode for Personal Meeting ID (PMI)



Require a passcode for Personal Audio Conference



Require passcode for participants joining by phone



#2 SET ENFORCEMENT LEVEL

Password

A password input field containing six dots, indicating a password of at least 6 characters.

i Passwords must be at least 6 characters.



Weak password

Password

A password input field containing six dots, with a red border around it, indicating a password that is too easy to guess.

*That password is too easy to guess. [Learn more](#)

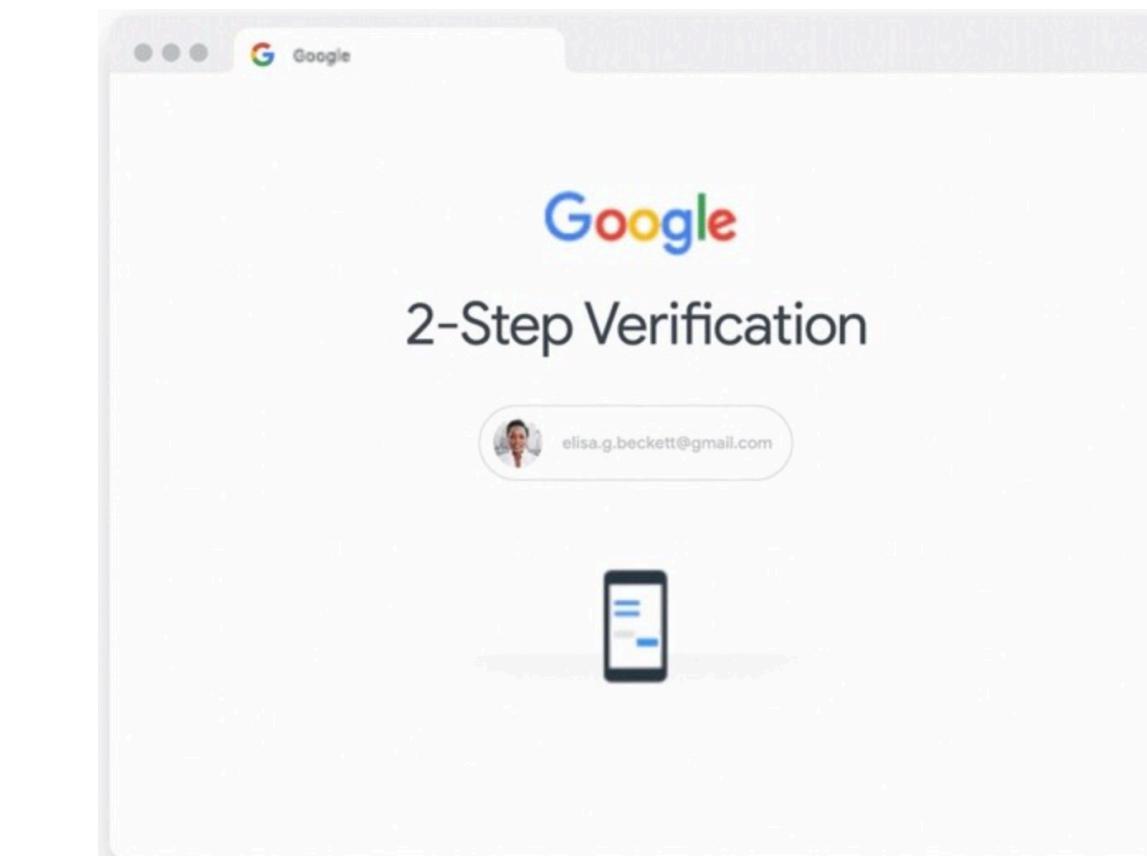
To continue, first verify it's you

An input field labeled "Enter your password" with a blue border.

Show password

[Forgot password?](#)

Next





Security Check-up

9 issues found

- ! Your devices
Fix 7 issues with your devices
- ! Recent security events
Review 1 critical event
- ! Third-party access
Review app passwords
- ✓ 2-Step Verification
2-Step Verification is on

Password Checkup
Check your 71 saved passwords for security issues



#3 ENCOURAGE

Take a minute to ensure you're keeping your Dropbox account protected.
Currently reviewing your **Dropbox Dropbox**. [Switch to Personal Dropbox](#).

1 Verify email

A current email address makes it easy to get back into your account if you ever forget your password.

Is [REDACTED] your current email?

Yes [Contact your team admin to change your email](#)

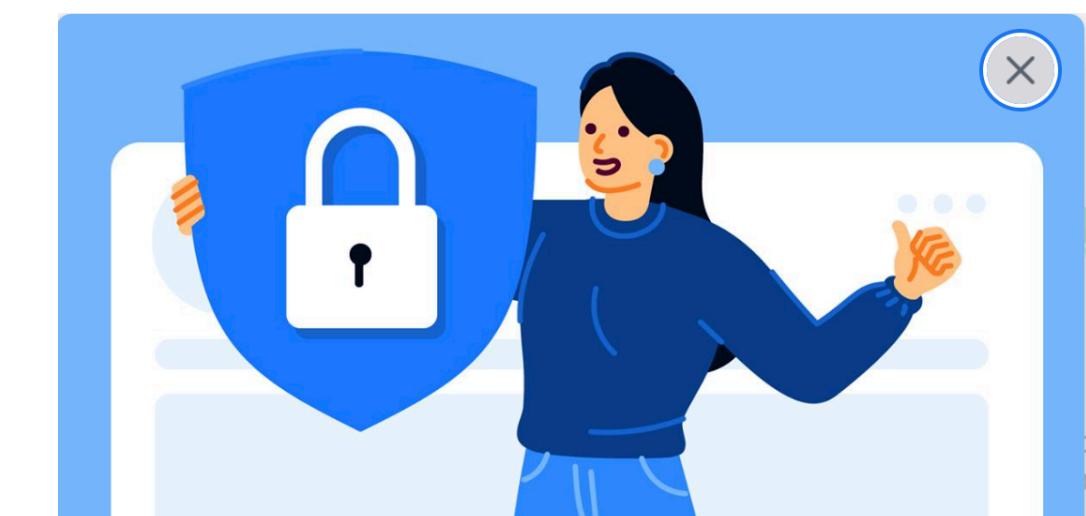
2 Review devices and browsers

3 Review linked apps

4 Ensure your password is secure

5 Review two-step verification settings

6 Try a password manager



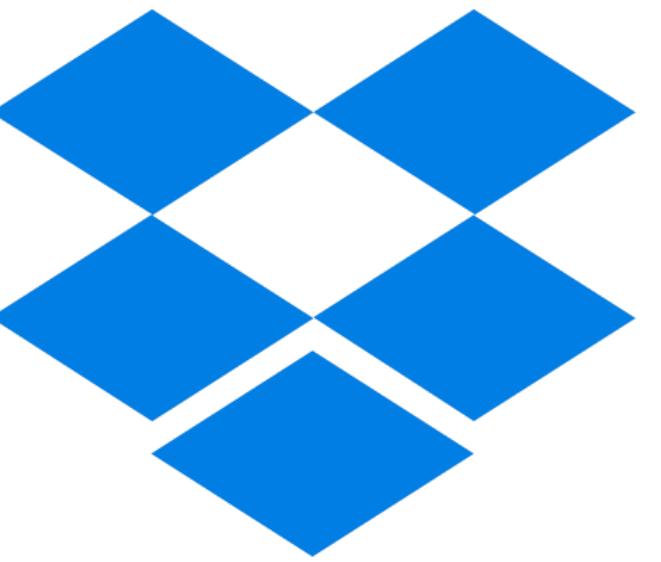
How to keep your account secure

You're all set. No security actions are recommended at this time.

- 🔑 Your password is OK
- 🔒 Turn on two-factor authentication
- 🔔 Login alerts are on

[Continue](#)

#4 DELEGATE (B2B)



#4 DELEGATE (B2B)

Settings > Two-step verification

The screenshot shows the 'Two-step verification' settings page. A blue box highlights the 'Optional for specific members' section, which contains the text: 'Optional for specific members' and 'Make enabling two-step verification optional for some members—even when it's required for the team.' To the right, a dropdown menu is open, showing three options: 'Optional' (selected), 'Optional' (disabled), and 'Required'. The 'Optional' option is described as 'Members can use two-step verification if they like'.

1 Two-step verification
Require an additional layer of security when signing in, like a key or code. [More about two-step verification](#)

Optional for specific members
Make enabling two-step verification optional for some members—even when it's required for the team.

Optional

✓ Optional
Members can use two-step verification if they like

Required
Members must use two-step verification

#4 DELEGATE (B2B)

Settings > Device approvals

Computers

How many computers can each member connect to Dropbox through the Dropbox desktop app?

Unlimited ▾

Unlimited

0

1

2

3

4

5

Remove

Mobile devices

How many phones and tablets can each member connect to Dropbox through Dropbox mobile apps?

Disconnected devices

What should happen when a member disconnects a computer or mobile device?

Device overages

#4 DELEGATE (B2B)

Settings > Web session control

Web session control

Set how long members can stay signed in to dropbox.com. They'll automatically be signed out when the session expires.

[Learn more](#)

Fixed session length

Set how long members can stay signed in to dropbox.com.

1 month ▾

1 day

1 week

2 weeks

✓ 1 month

Idle session length

Set how long members can be idle for while signed in to dropbox.com.

ADMIN CONTROL - OUR COMPETITORS

Password Requirements

Character settings: Minimum required characters:

Require number(s):

Require special character(s):

Require at least one uppercase letter

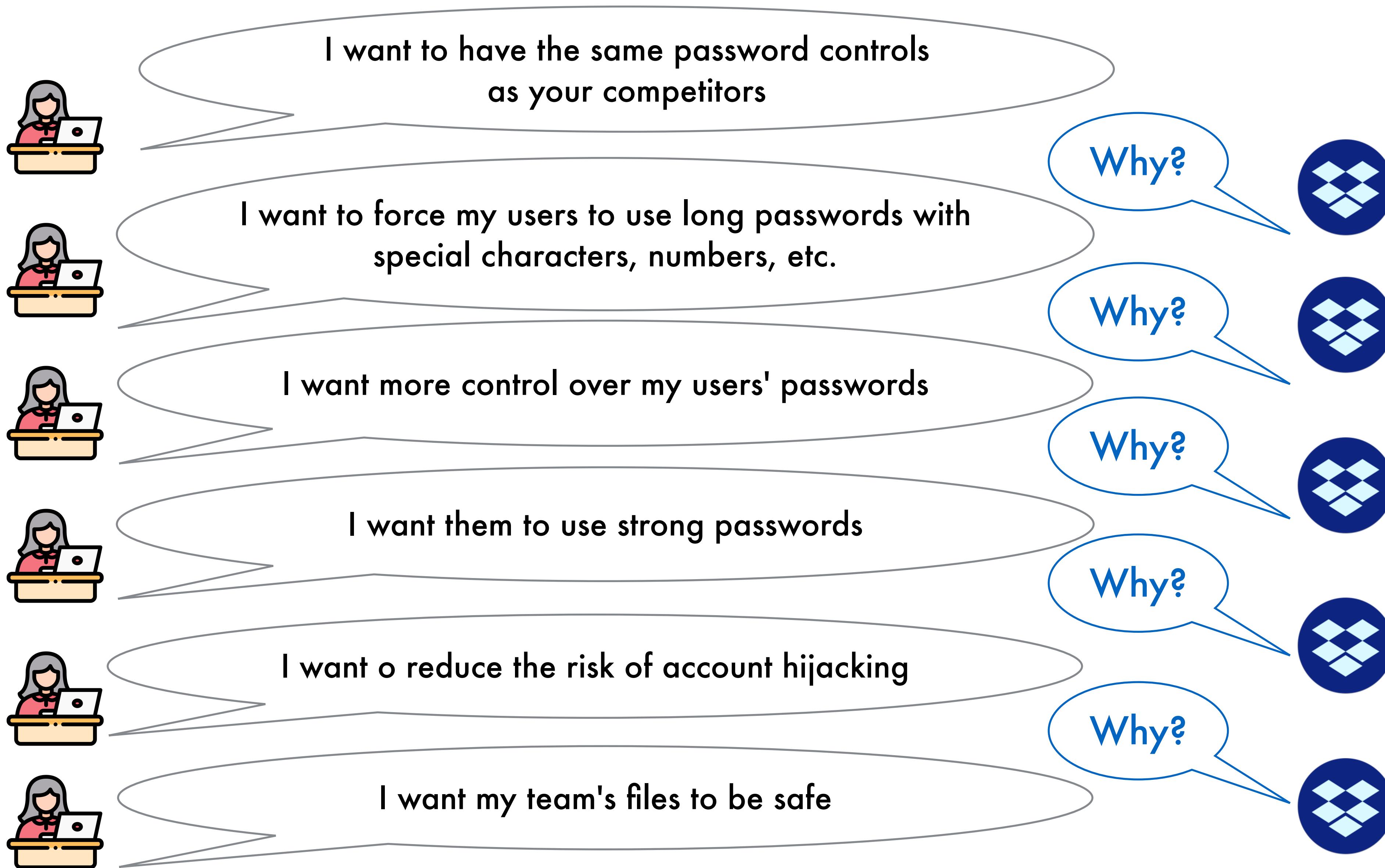
Prevent common words / email address as a password:

Password resets: Require users to reset passwords every:

Perform a global password reset now.
All users and admins will be required to change their password on next login.
Reset Passwords Now

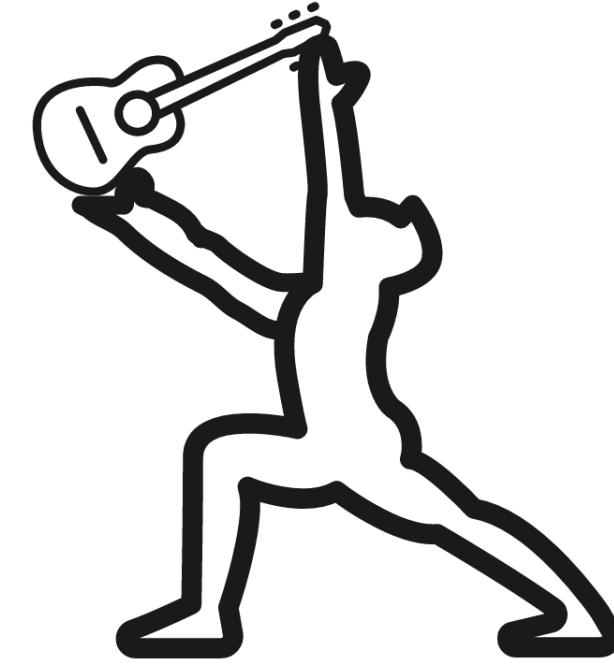
Prevent reusing passwords from: Last times

5 WHY'S

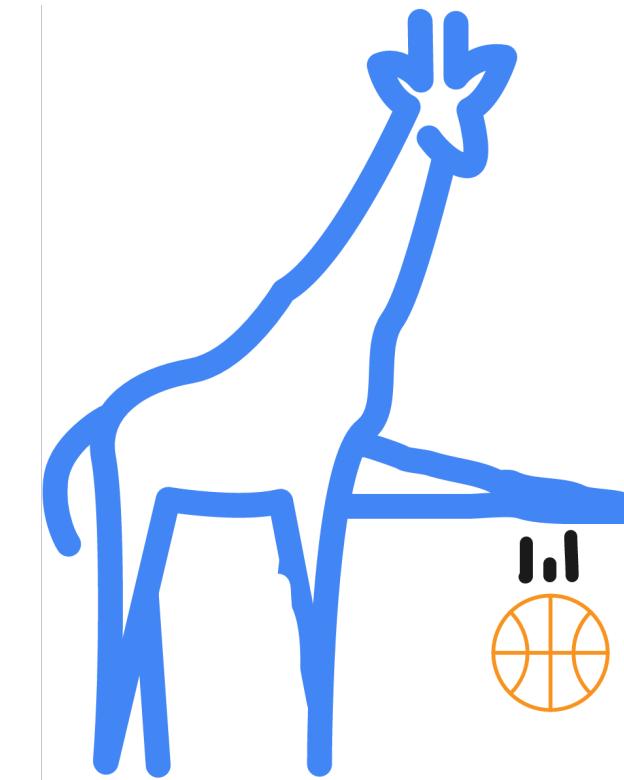


WHICH PASSWORD IS BETTER?

Tr0ub4dor&3



bluegiraffeplaysball



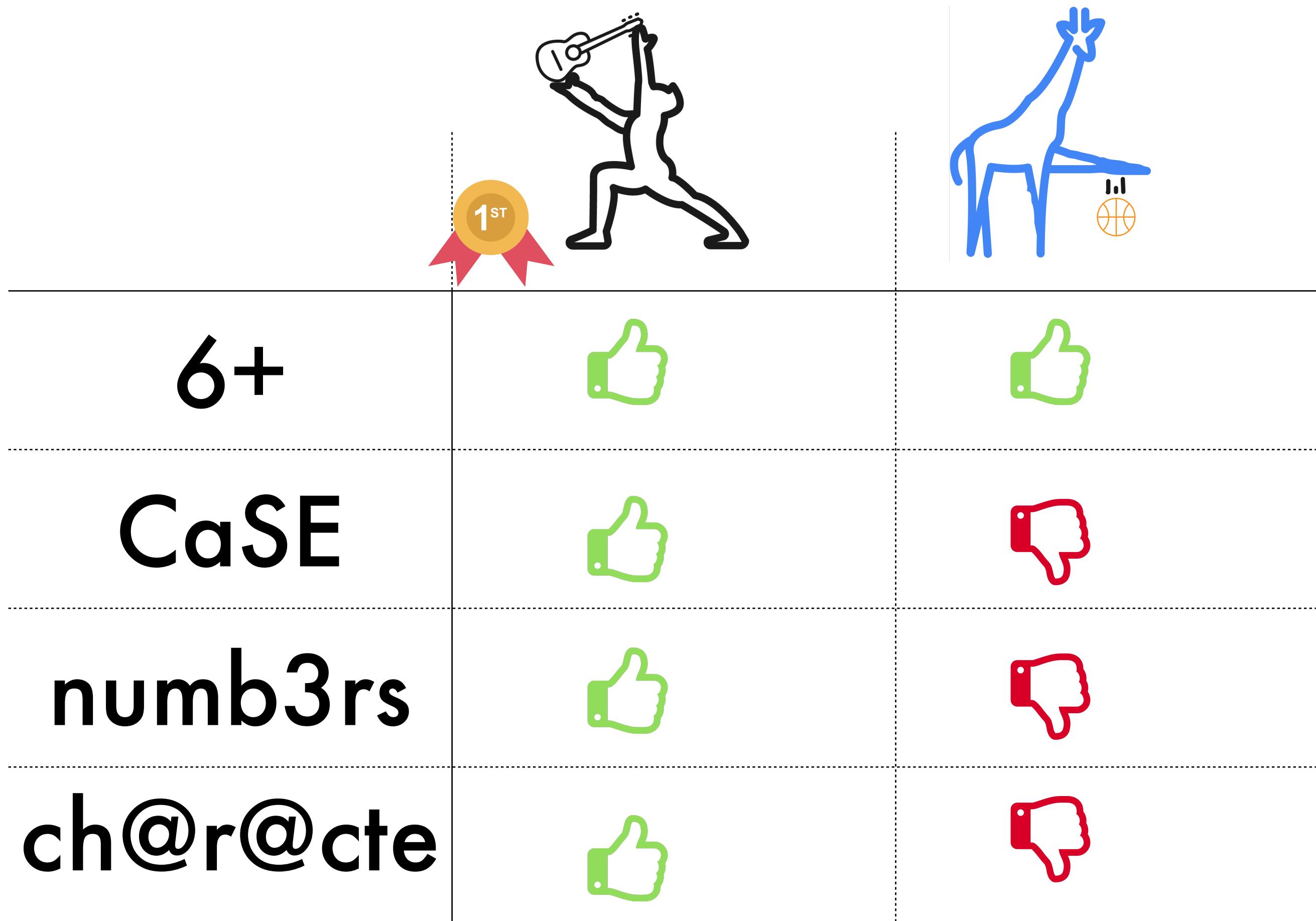
GOOD PASSWORD



A **strong password** consists of at least six characters (and the more characters, the stronger the **password**) that are a combination of letters, numbers and symbols (@, #, \$, %, etc.) if allowed. **Passwords** are typically case-sensitive, so a **strong password** contains letters in both uppercase and lowercase.

- 6+ characters
- MiXEd CaSE
- numb3rs
- special ch@r@cters!

LET'S COMPARE





Open sesame!

Your username
or password are
incorrect.

Op3n \$e\$ame?



DODN
© 2014
BIZARRO.
5.17.14

[Facebook.com/BizarroComics](https://www.facebook.com/BizarroComics) Dist. by King Features

Hard to guess



Easy to remember

HARD TO GUESS

of guesses required
to crack the password

NAIVE ESTIMATION

guesses = cardinality ^{length}



Cardinality	abc	26	→	abc+ABC+123+@\$%	95
Guesses	vxcblt	26^6	→	d%ac3?	95^6
1000/sec.	⌚ 15 days		→	⌚ 140 years	

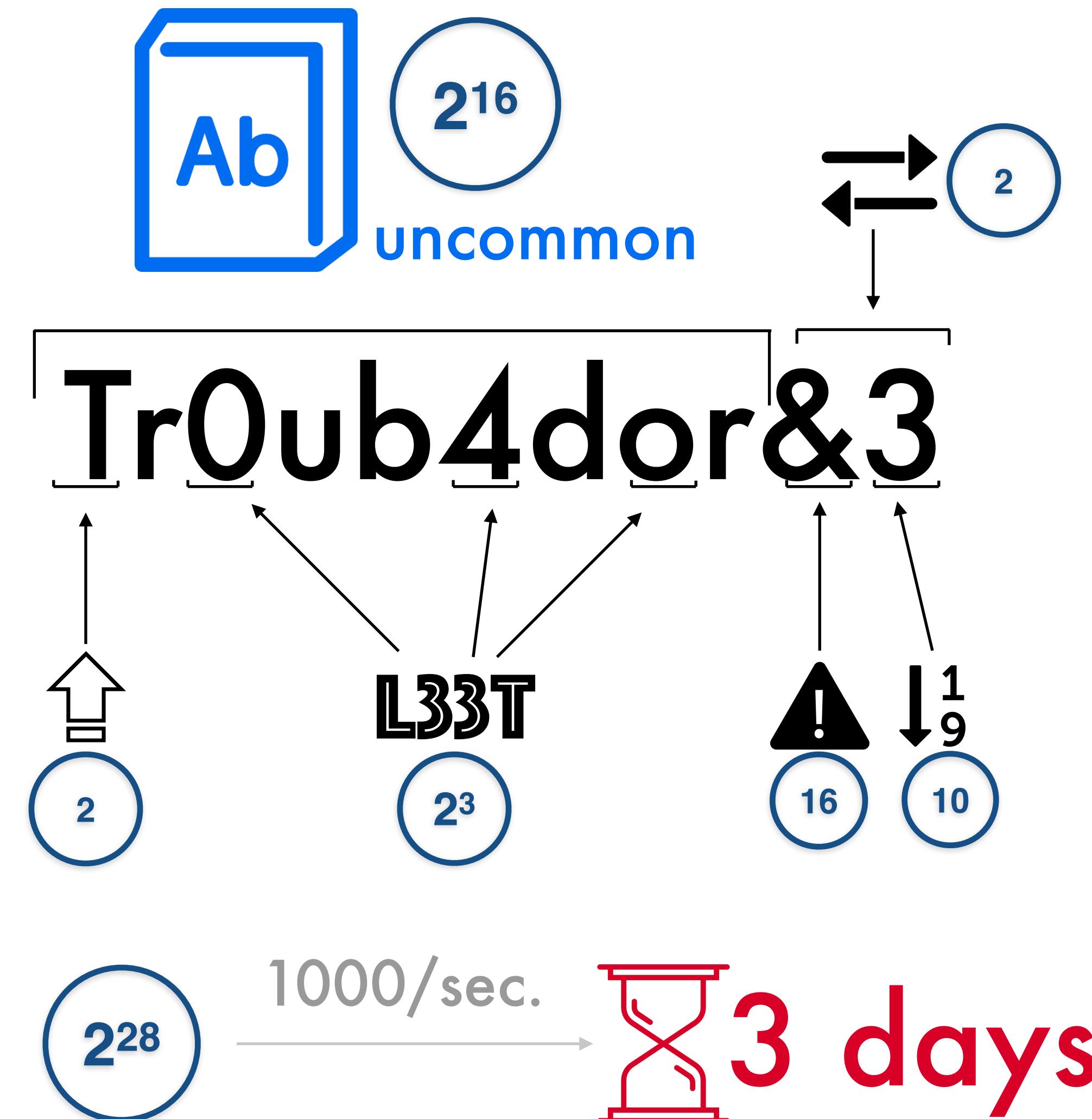
length
cardinality

We're humans

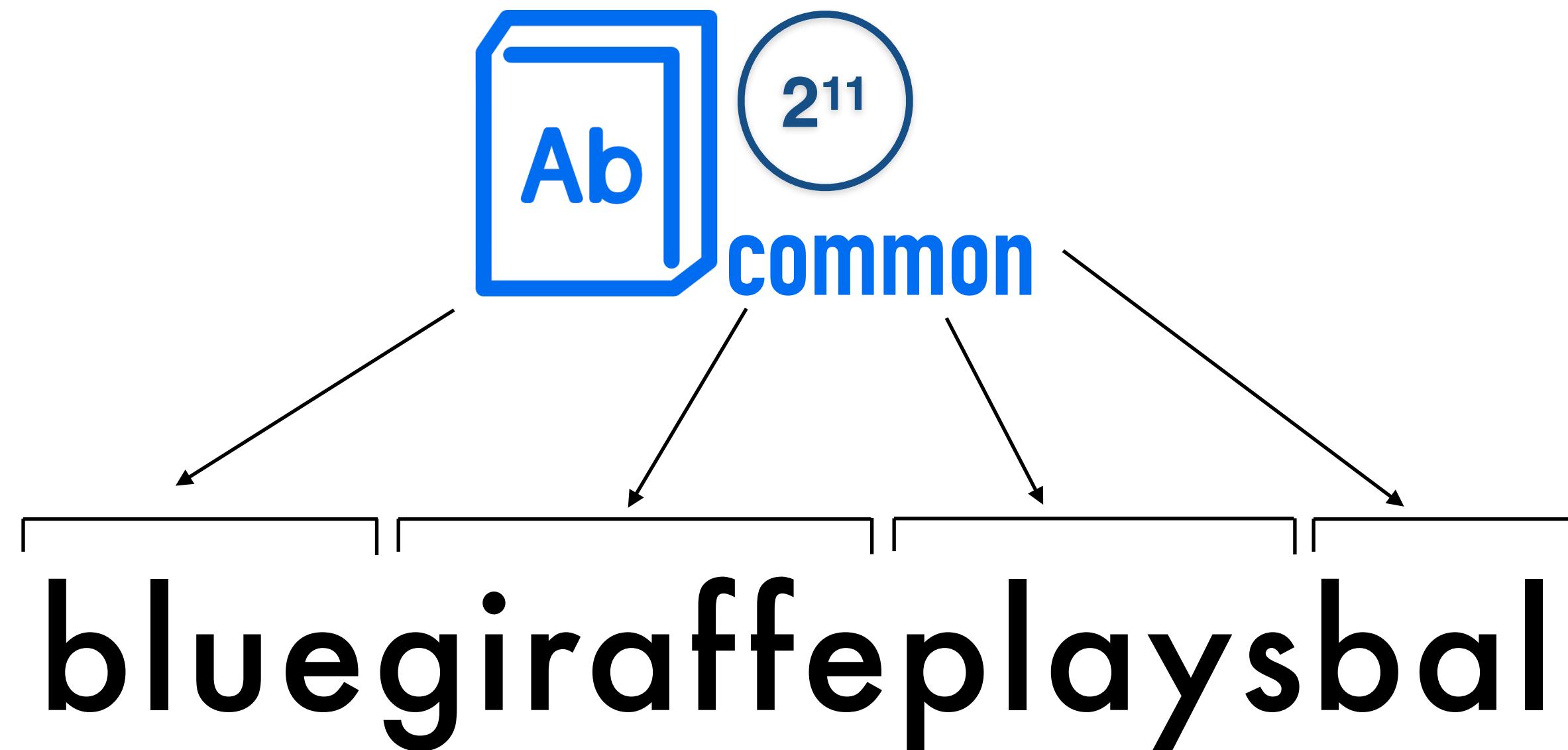


Not robots

HARDER TO GUESS



HARDER TO GUESS



A diagram showing the relationship between password entropy and cracking time. A blue circle contains the text '2⁴⁴'. An arrow labeled '1000/sec.' points from this circle to a green hourglass icon. To the right of the hourglass, the text '550 years' is written in green.

EASY TO REMEMBER

Tr0mbone?3

Troubad0r?3

Tr0ubador?3

Tr0ub4d0r!3

Tr0ubad0r?3

Tr0ub4d0r&3

:0



BIGGEST SITES ESTIMATIONS

1 2 16
password123456!
19 1000/sec. seconds



Password strength: Strong

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. [Why?](#)

Create a password

.....

Confirm your password



New

Password strength: Strong



.....

—

✓



.....

confir

Your password must have:

- 8 or more characters
- Upper & lowercase letters
- At least one number

Security

Strength: strong

IF WE ONLY HAD A TOOL

Password to test: **Break it down!**

Estimating strength of password "password123456!":

```
Approx time to crack: instant  
(in seconds): 0  
Strength score (1-5): 1  
Entropy estimate (bits): 3
```

password:

```
pattern: dictionary  
token: password  
rank: 1  
entropy: 0
```

123456:

```
pattern: dictionary  
token: 123456  
rank: 2  
entropy: 1
```

! :

```
pattern: dictionary  
token: !  
rank: 2  
l33t_entropy: 1  
entropy: 2
```

WE DO HAVE!

zxcvbn 

Built @  2012 by Dan Wheeler

Open-sourced on  under MIT license

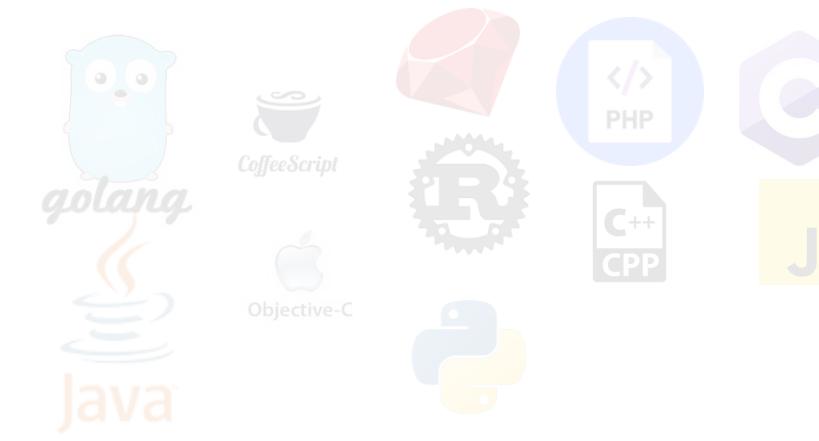
10K+ 

HOW TO USE

```
$ npm install zxcvbn  
  
$ node  
  
> var zxcvbn = require('zxcvbn');  
  
> zxcvbn('Tr0ub4dour&3');
```

FAST & LIGHT

</> Implemented in:



⌚ Fast: ~5-20ms for up to 25 characters

⚖️ Lightweight: code:<50kb; data:<1mb;

BILL BURR REGRETS

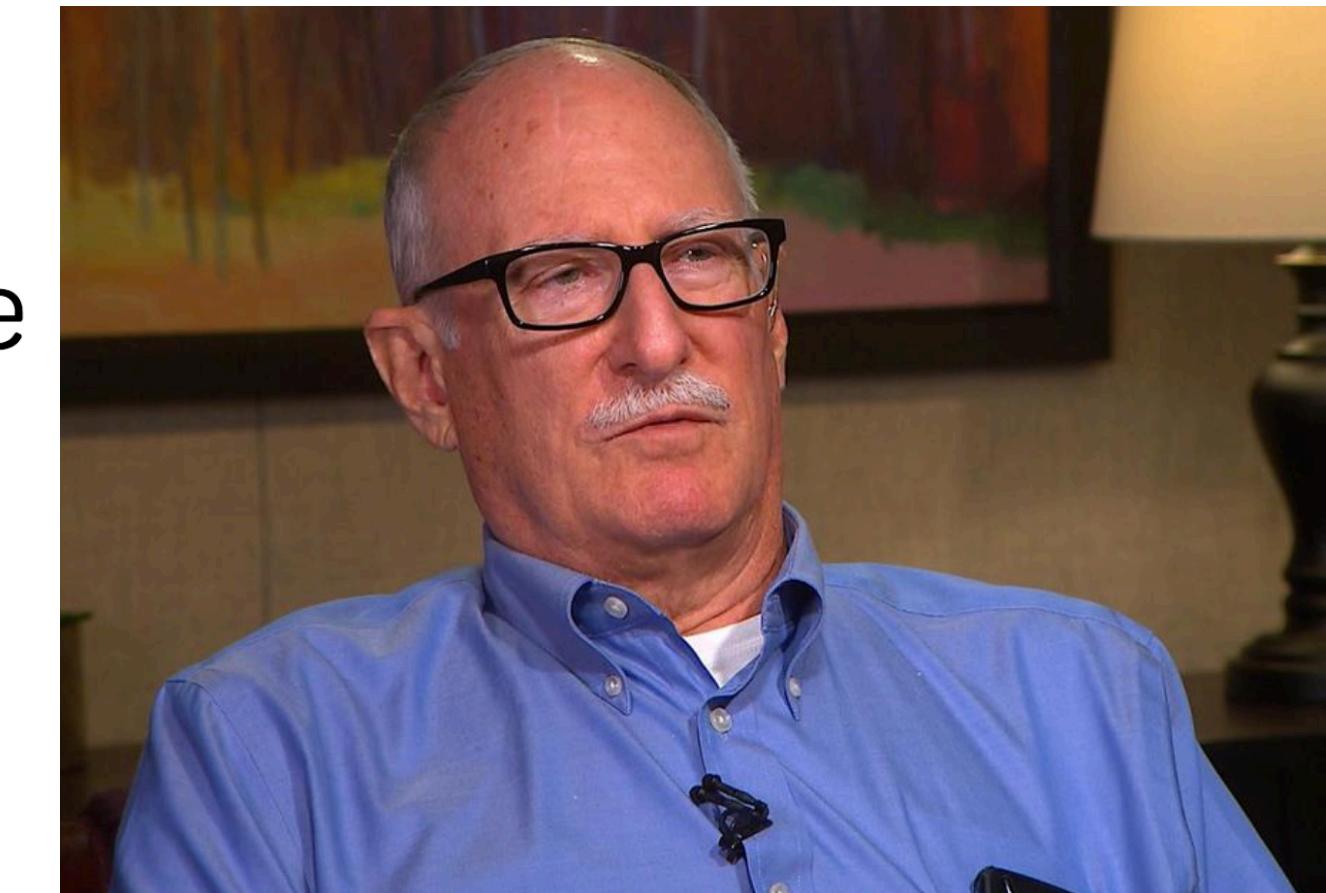


REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

SECURITY

Father of passwords regrets the advice he gave

Commentary: Bill Burr thought he gave the right advice about password creation. He's decided he was wrong.



USA TODAY

NEWS SPORTS LIFE MONEY TECH TRAVEL OPINION 83° CROSSWORDS VIDEO GRATEFUL SUBSCRIBE NEWSLETTERS STOCKS N

Password expert says he was wrong: Numbers, capital letters and symbols are useless



POLITICS BORDER CRISIS TECH & MEDIA BUSINESS INTERNATIONAL THINK

SECURITY

Forget Everything You Know About Passwords, Says Man Who Made Password Rules

The Telegraph

HOME NEWS SP

Technology Intelligence

Gadgets | Innovation | Big Tech | Start-ups | Politics of Tech | Gaming | Podcast | Te

▲ > Technology Intelligence

Password guru who told the world to make them complicated admits: I got it completely wrong

RECOMMENDATION UPDATE - NIST*

- No password hints**
- Knowledge-based authentication (KBA) is out.**
- No more expiration without reason**
- No composition rules**

*National Institute of Standards and Technology

ADMIN CONTROL - OUR COMPETITORS

Password Requirements

Character settings: Minimum required characters:

Require number(s):

Require special character(s):

Require at least one uppercase letter

Prevent common words / email address as a password:

Password resets: Require users to reset passwords every:

Perform a global password reset now.
All users and admins will be required to change their password on next login.
Reset Passwords Now

Prevent reusing passwords from: Last times

Password strength

Require your team to set stronger passwords on their Dropbox accounts.

Strong ▾

WIN, WIN, WIN

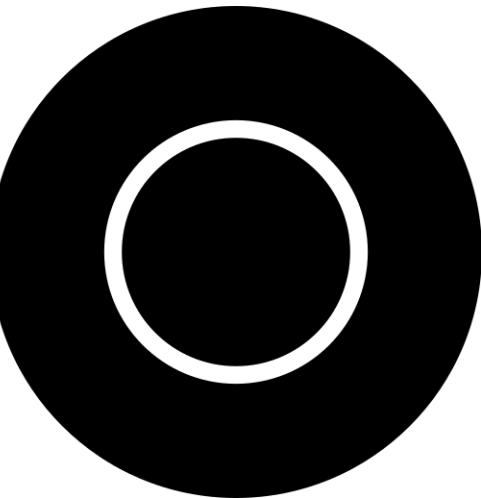
Password strength

Require your team to set stronger passwords on their Dropbox accounts.

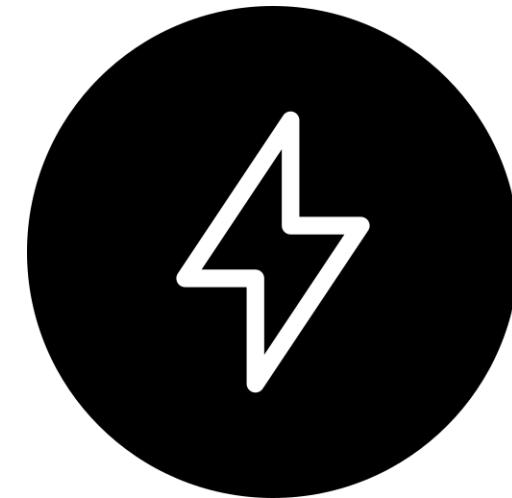
Strong ▾



Fast



Simple

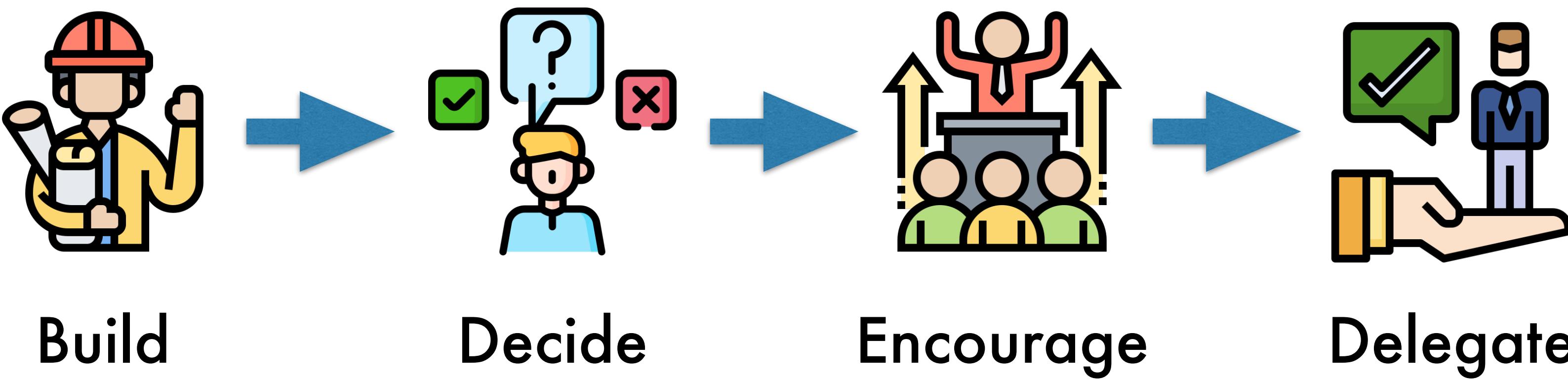


Powerful

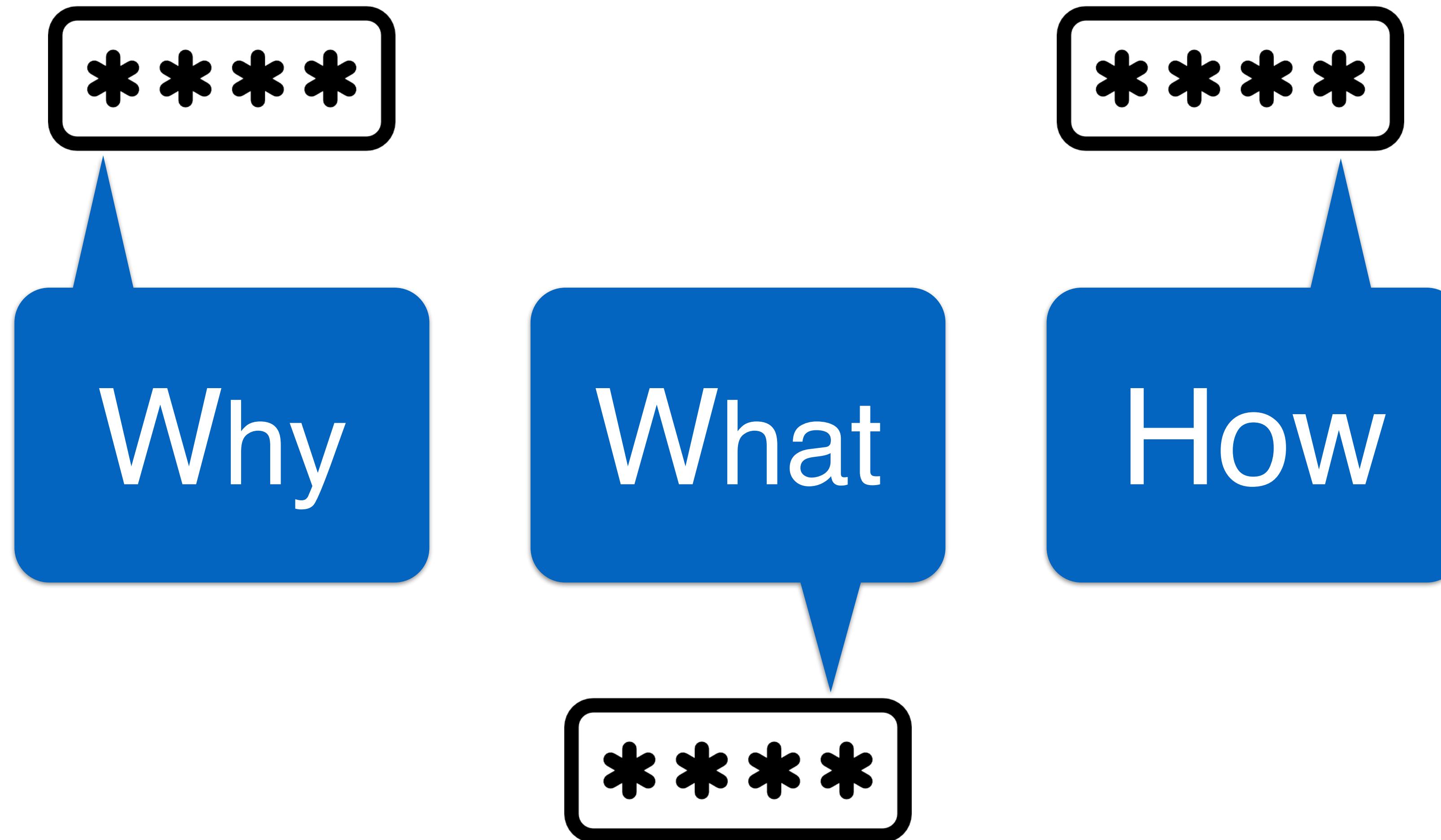
CONCLUSION



FINDING THE BALANCE



PASSWORD ESTIMATION



SECURITY VS. UX

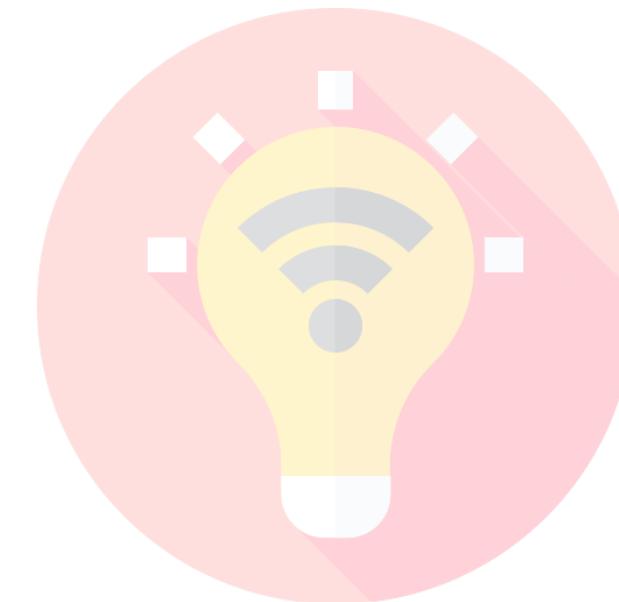
Don't automatically build



5 Whys



Smart algorithm

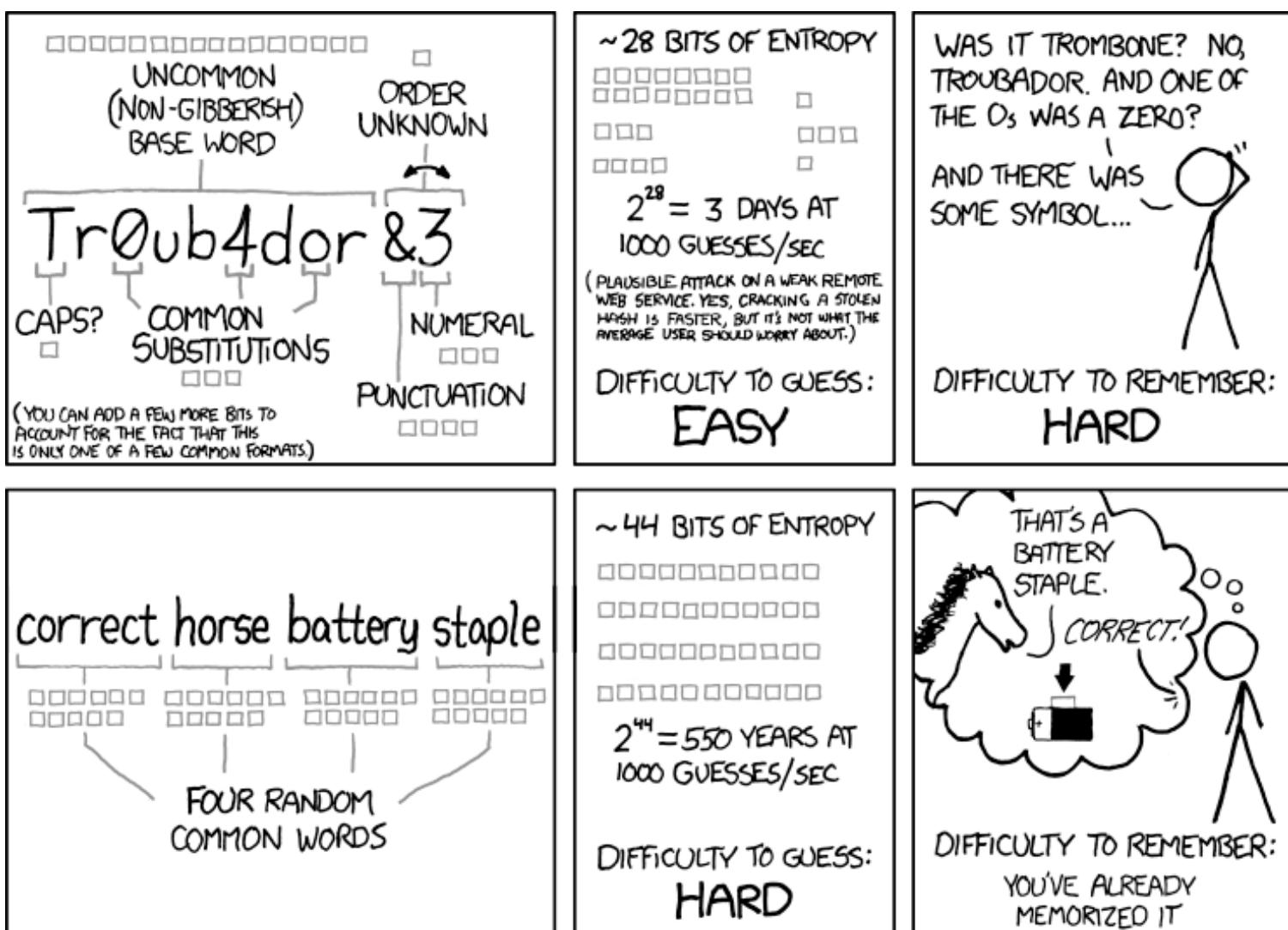


Early conversation



THANK YOU

XKCD



Dan Wheeler

A screenshot of a GitHub repository page for `dropbox/zxcvbn`.

The repository has the following statistics:

- Code: 265
- Issues: 96
- Pull requests: 26
- Actions: 0

The master branch is selected. Recent commits include:

- lowe Fix broken demo link in README (Oct 13, 2017)
- data-scripts doc tweak: make usage in data-scripts con... (6 years ago)
- data skip non-unicode top passwords in xato. (t... (6 years ago)
- demo add password feedback to demo (6 years ago)



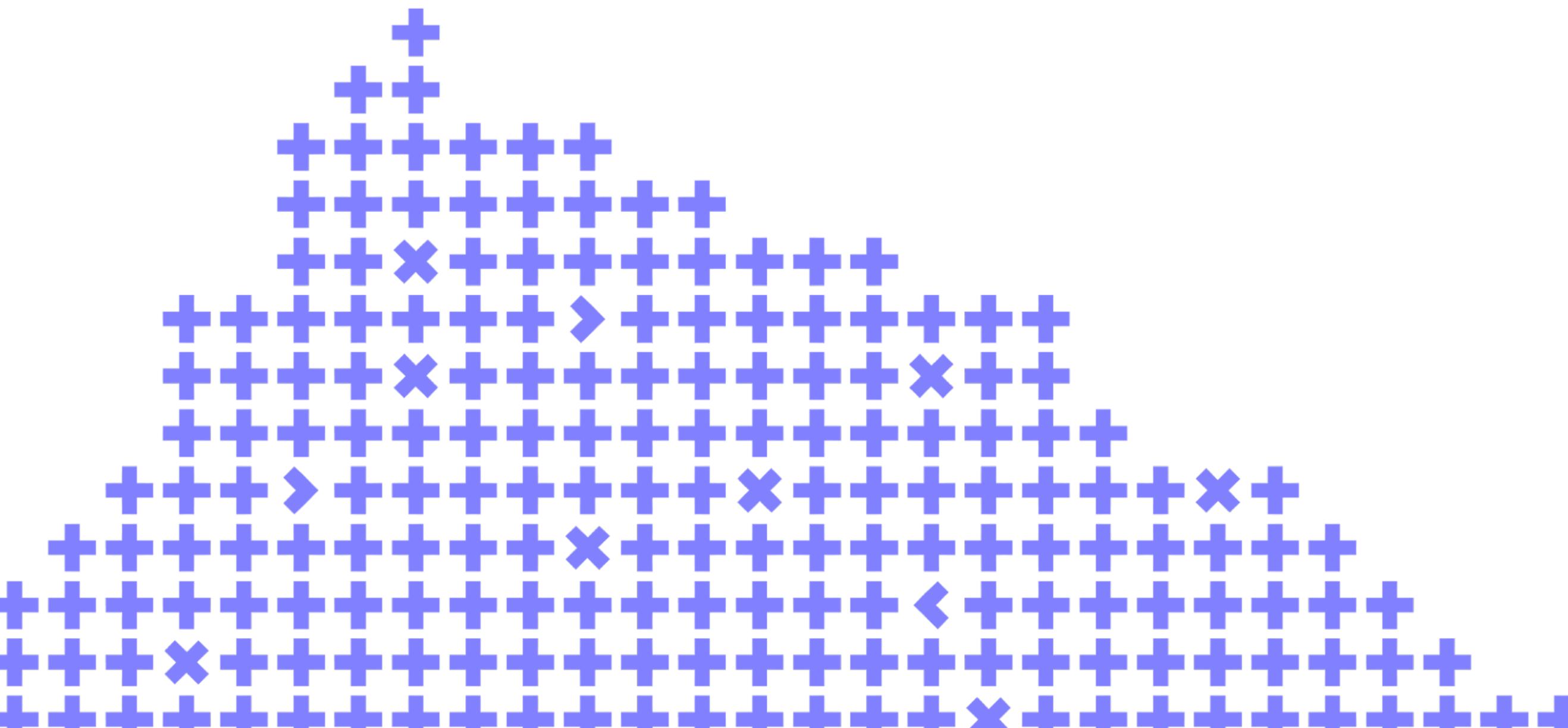
KEEP
CALM
AND
FINISH
HIM

THANK YOU



Alon Kiriati

Leave your feedback! You
can rate the talk and tell
me what you've liked and
what can be improved :)



Co-organizer

Yandex